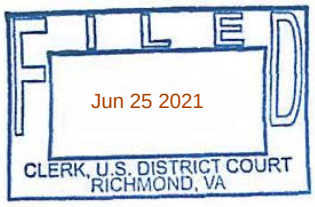
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



IN THE MATTER OF THE SEARCH OF: **Apple iPhone 11 Yellow 64GB,** **IMEI 356547109384289**	Case No. 3:21-sw-90 **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, Melvin Gonzalez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed by the FBI for over fifteen years. I am currently assigned to the Richmond Field Office, Richmond, VA. I am assigned to the Child Exploitation Task Force, which conducts investigations pertaining to child sex trafficking, child pornography, and child abductions. I have received training from the FBI in the areas of child exploitation. I was previously assigned for six years to the San Juan Field Office, where I investigated violent crimes, gangs, and drug trafficking. During my career in law enforcement, I have received extensive training in the conduct of a variety of investigations, including drug investigations, organized crime, violent crime, white collar crime, and others. In the course of my employment as a sworn law-enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18 of the United States Code, including § 2251, involving production of child pornography, § 2252A, involving a variety of child exploitation and child pornography offenses, and § 2422, involving online enticement or coercion of a minor to engage in illegal sexual activity.

2. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. As a Special Agent, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. This affidavit is submitted in support of a search warrant authorizing the seizure and examination of an Apple iPhone 11 Yellow 64GB, IMEI 356547109384289 (hereinafter "SUBJECT DEVICE"), wherever that SUBJECT DEVICE may be located. The SUBJECT DEVICE to be searched is more particularly described in Attachment A, which is incorporated herein by reference.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) Distribution or Receipt of Child Pornography, 18 U.S.C. § 2252A(a)(5)(A) Possession of Child Pornography, 18 U.S.C. § 2251, Production of Child Pornography, and 18 U.S.C. § 2251A Buying and Selling of Children are located on the SUBJECT DEVICE described in Attachment A. There is also probable cause to search the SUBJECT DEVICE described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is "a district court of the United States … that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

7. **Receipt and Distribution of Child Pornography:** 18 U.S.C. § 2252A(a)(2)(A) and (B) provides that it is unlawful for any person to knowingly receive or distribute a visual depiction of sexually explicit conduct, wherein the depiction involved the use of a minor, a computer image of a minor or indistinguishable from that of a minor, or a computer image created, adapted, or modified to appear as an identifiable minor, and in which the depiction was moved in interstate commerce, including by computer, and the person knew that the depiction contained such child pornography.

8. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5)(B) provides that it is unlawful for any person to knowingly possess any matter that contains an image of child pornography that had been transported in interstate commerce by any means, including by computer, or had been produced using materials that had been transported in interstate commerce by any means, including by computer, and the person knew the matter contained such child pornography.

9. **Production of Child Pornography:** 18 U.S.C. § 2251(a) provides that it is unlawful for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in…any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct…if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce.

10. **Selling or Buying of Children:** 18 U.S.C. § 2251A provides that it is unlawful for any parent, legal guardian, or other person having custody or control of a minor to sell or otherwise transfer custody or control of such minor or offer to sell or otherwise transfer custody of such minor either—…(2) with the intent to promote either—(A) the engaging in of sexually

explicit conduct by such minor for the purpose of producing any visual depiction of such conduct; or (B) the rendering of assistance by the minor to any other person to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

Probable Cause

11. From November 18, 2020 to November 24, 2020, an Online Covert Employee ("OCE") conducted undercover chat sessions on the application Kik as part of an ongoing investigation by the Federal Bureau of Investigation (FBI) Philadelphia Field Office. During the undercover sessions, the OCE conducted an account takeover of Kik account "twistedtazz." This Kik Account was a member of the private Kik group PedMoms Premium. The owner of PedMoms Premium was listed as PedSeller02, and the administrator was listed as PedSeller01. The owner and administrator of a group are the only users who can accept, remove, or ban members of the group.

12. While in the PedMoms Premium group, the OCE observed several members sharing images and videos constituting child sexual abuse material (CSAM). As used here, CSAM has the same definition as Child Pornography (any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8). For example, one member posted a video of minor female lasciviously exposing her vagina. Another member posted a video of a prepubescent female being raped.

13. The OCE, acting as twistedtazz, engaged in conversation with PedSeller02 (Miss Linsay) about meeting an 11-year-old for sex. PedSeller02 requested 50% down payment to

provide the 11-year-old and provided CashApp name $KittyCorner8 as well as an address and phone number. PedSeller02 banned the OCE from the private group after the OCE asked about the validity of the offer. PedSeller02 then added the OCE to a private chat with multiple members. In the private chat, one member redneckin515 (Jonn jonn) advised that the offer for sex with children was a scam and not to pay her.

14. Based on information collected during the undercover activity and communications, PedSeller02 also requested payments to her CashApp account $KittyCorner8 in order for other users to gain access to files containing CSAM.

15. Pursuant to a subpoena, on November 23, 2020, MediaLab, owner of Kik Messenger, provided records associated with Kik account PedSeller01, which indicated the following:

First Name: Miss
Last Name: Lauren
Email: pekifil237@anyqx.com (confirmed)
Username: pedseller01

16. MediaLab also provided the following recent IP addresses for the Kik Account PedSeller01: Recent IPs: 2020/11/11 19:30:22 UTC 1605123022820 CAN "ip":"199.58.83.9", "remotePort":"56762", "chatNetwork":"WIFI" - Koumbit, Montreal, Canada 2020/11/11 15:58:37 UTC 1605110317666 CAN "ip":"170.82.211.95", "remotePort":"59992", "chatNetwork":"WIFI" - Digicel, Trinidad and Tobago.

17. Pursuant to a subpoena, on November 30, 2020, MediaLab provided records associated with Kik account PedSeller02, which indicated the following:

First Name: Miss
Last Name: Linsay
Email: rehdeheheje@ahah.com (unconfirmed)
Username: pedseller02

18. MediaLab also provided the following recent IP addresses for the Kik Account PedSeller02: Recent IPs: 2020/10/25 17:16:08 UTC 1603646168242 CAN "ip":"170.82.211.95", "remotePort":"50040", "chatNetwork":"WIFI" - Digicel Trinidad 2020/10/25 21:45:17 UTC 1603662317765 CAN "ip":"199.58.83.9", "remotePort":"45106", "chatNetwork":"WIFI" - Kombit, Canada 2020/10/27 02:55:16 UTC 1603767316304 CAN "ip":"37.218.241.105", "remotePort":"33506", "chatNetwork":"WIFI" - Greenhost, Netherlands 2020/11/16 19:59:21 UTC 1605556761350 CAN "ip":"200.7.90.129", "remotePort":"39181", "chatNetwork":"WIFI" - Digicel, Trinidad 2020/11/22 06:12:45 UTC 1606025565185 CAN "ip":"161.0.155.212", "remotePort":"46890", "chatNetwork":"WIFI" - Digicel, Trinidad 2020/11/22 09:40:39 UTC 1606038039356 CAN "ip":"181.118.37.155", "remotePort":"47174", "chatNetwork":"WIFI" - Digicel, Trinidad.

19. The above referenced IP addresses collected via subpoena, revealed the potential usage of anonymization techniques utilizing tools such as Virtual Private Networks (VPN) to avoid being associated with a specific location and internet provider given that the IP addresses are associated with different countries across the globe.

20. Pursuant to a subpoena, on December 3, 2020, Square provided records related to the Cashapp account associated with $KittyCorner8. The subscriber records identified the owner of the account as Jessica Lynn Tanner, date of birth April 4, 1999, address 8800 Merseyside Lane, Chesterfield, VA 23832, telephone number 804-836-8629 “SUBJECT DEVICE’s NUMBER”, email address jesstan5159@gmail.com, bank cards xxxxxxxxxxxx1251 (Virginia Credit Union, Inc.) and xxxxxxxxxxxx3582 (SunTrust Bank). The transaction records showed several transactions in the amount of $5 associated with usernames from members of the PedMoms Premium group. The list of transactions for the

account identified from the subpoena indicated the use of an iPhone device to access the Cashapp account.

21. According to the Virginia Department of Motor Vehicles (DMV) Tanner is not licensed in the state of Virginia but possesses a Virginia State identification card. According to other searches conducted by the FBI, Tanner does not have vehicles or properties associated with her.

22. During an open social media search, Facebook account jessican.tanner.186 was identified as being used by Tanner. According to Tanner's Facebook account, Tanner is listed as a lead teacher at the Woodlake Child Development Center since March 2019. According to the Virginia Employment Commission (VEC), Tanner is employed by Tuckaway Inc. Based on open source search, Woodlake Child Development Center is administered by Tuckaway Inc.

23. In order to attempt to identify Tanner's residence, agents served additional subpoenas.

24. Pursuant to subpoena results from February 22, 2021 and May 12, 2021, Verizon Wireless provided limited records pertaining to cellular device 804-836-8629. Account activity to include call detail records were received from Verizon Wireless. Verizon Wireless described the device associated with 804-836-8629, as an Apple iPhone 11 Yellow 64GB. Verizon also identified that the cellular device is assigned International Mobile Subscriber Identity (IMSI) 311480392114564 and International Mobile Equipment Identity (IMEI) 356547109384289. The IMSI and IMEI are unique numbers that identify the particular SIM card (IMSI) and the actual mobile device (IMEI) for the cellular device. Verizon Wireless advised that TracFone Inc. was in possession of subscriber and billing information for the cellular device.

25. Pursuant to a subpoena on March 17, 2021, Virginia Credit Union provided the following information for bank card xxxxxxxxxxxx1251:

- Account Name: Jessica L Tanner
- Address: 12311 Sandbag Rd, Midlothian, VA 23113

26. Pursuant to a subpoena on March 30, 2021, SunTrust Bank (TRUIST Financial) provided the following information for bank card xxxxxxxxxxxx3582:

- Account from McDonough, GA reported U-Stolen and closed

27. Pursuant to a subpoena on May 10, 2021, Verizon Wireless provided the following information for IPs used to log into Tanner's Facebook account: Verizon Natting IPs (which could be used by numerous users at the same time):

- 174.251.128.92 Time 2021-04-12 16:34:30 UTC (Your Affiant reviewed the records provided by Verizon Wireless and identified the following IP associated with Tanner's Cellular Records)
- 174.251.136.13 Time 2021-01-23 08:10:05 UTC
- 174.251.136.207 Time 2020-12-07 22:13:16 UTC

28. Pursuant to a subpoena on May 12, 2021, Verizon FIOS provided the following information for an IP used to log into Tanner's Facebook account on 04/13/2021:

- IP Address: 2600:4040:1332:5500:59f3:3d4:b5eb:3dbe , Customer Name: Drummond, Account Address: 11904 Winterpock Rd, Chesterfield, VA 238380

29. Based on the review and analysis of the above-mentioned facts Agents were unable to determine a specific residence location for Tanner.

30. Agents obtained call detail records (CDRs) with cell site location information (CSLI) from Verizon for Tanner's phone, telephone number 804-836-8629, for the period of November 18, 2020 through May 21, 2021. The CDRs were provided to FBI's Cellular Analysis Survey Team (CAST), who analyzed the records to determine the approximate locations of the phone for the duration of the records. The CDRs indicated that, of the 357 records that contained CSLI, the top three locations identified were:

a. A cluster of three cell sites and sectors used to make or receive 186 calls (approximately 52%) and is consistent with providing coverage to the area of the 15211 Beach Road, Chesterfield, Virginia 23838.

b. A cluster of two cell sites and sectors used to make or receive 64 calls (approximately 18%) and is consistent with providing coverage to the area of 12311 Sandbag Road, Midlothian, Virginia.

c. A cluster of two cell sites and sectors used to make or receive 55 calls (approximately 15%) and is consistent with providing coverage to the area of the Tuckaway Woodlake Child Development Center at 14750 Meyer Cove Drive, Midlothian, Virginia.

31. In addition to CDRs, you affiant obtained additional records for the period of May 24, 2021 through June 2, 2021 that include CSLI as well as an approximate distance Tanner's phone was from the cell site, also known at RTT records. The RTT records were also provided to FBI's CAST, who analyzed the records to determine the approximate locations for the phone for the duration of the records. The RTT records indicated that:

a. On the evenings and overnight hours of May 24 – 27, 2021 and May 31, 2021, the RTT records and the distance from the tower measurements included the area of the 15211 Beach Road, Chesterfield, Virginia 23838.

b. On the evenings and overnight hours of May 28 – 30, 2021, the records and the distance from the tower measurements included the area of 12331 Sandbag Rd, Midlothian, Virginia;

c. On the days of May 25 – 28, 2021 during, but not limited to, the hours from 1:00 pm – 6:00 pm, the RTT records and the distance from the tower

measurements included the area of the Tuckaway Woodlake Child Development Center at 14750 Meyer Cove Drive, Midlothian, Virginia.

32. On June 2, 2021, Agents conducted a physical surveillance in the vicinity of the 15211 Beach Road, Chesterfield, Virginia 23838. During the surveillance, Agents observed a female individual matching the description of Tanner exiting the front door of the residence with an unidentified male and entering a vehicle parked in the driveway. The vehicle then exited the driveway with the male driving and the female in the front passenger seat. Approximately thirty minutes later, Agents observed the same vehicle at the Woodlake Child Development Center at14750 Meyer Cove Drive, Midlothian, Virginia 23112. The female exited the vehicle and entered the Woodlake Child Development Center.

TECHNICAL TERMS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Smartphone** is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as “apps.” Smartphones can access the

Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

b. "**Internet Protocol address**" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. **Storage medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

e. "The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides,

negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

34. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter, "collectors").

35. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

36. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

37. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

38. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

39. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

40. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

41. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in

that location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

42. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Examples of such devices providing a fingerprint unlocking capability are several models of Apple's iPhone, as well as several phones, including but not limited to the Samsung Galaxy, which use the Android operating system. Apple iPhones may be fingerprint unlocked using a function called Touch ID, which during setup allows for registering as many as five (5) fingerprints to unlock the device. Samsung's Galaxy S8 and S8+ models may be configured to be unlocked with as many as four (4) fingerprints. In fact, the number of electronic devices providing a fingerprint unlocking capability, including both smart phones and laptops, is growing continually. If a device is equipped with a facial recognition feature, a user may enable

the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based upon the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

43. In my training and experience, users of electronic devices often enable the above-mentioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. In some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

44. Related to the above discussion regarding encryption, if a forensic examination is not conducted shortly after seizing the device while it is in an unlocked state, or unlocking the device using biometric features immediately upon seizing it, law enforcement investigators may completely lose the ability to forensically examine the device, assuming the device's owner refuses to disclose the password. The passcode or password that would unlock any such device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by this warrant.

45. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using

Touch ID when: 1) more than 48 hours has elapsed since the device was last unlocked; or 2) when the device has not been unlocked using a fingerprint for eight (8) hours *and* the passcode or password has not been entered in the last six (6) days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four (4) hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

46. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of these biometric features, the warrant I am applying for would permit law enforcement personnel to: 1) press or swipe the fingers (including thumbs) of TANNER, to the fingerprint scanner of the device(s); and/or 2) hold the device(s) in front of the face of TANNER and activate the facial recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. In the event that law enforcement is unable to unlock the subject device(s) within the number of attempts permitted by the pertinent operating system, this will simply result in the device(s) requiring the entry of a password or passcode before it can be unlocked.

47. Due to the foregoing, I request that the Court authorize law enforcement personnel to press the fingers (including thumbs) of TANNER to unlock the SUBJECT DEVICE so that investigators may conduct the search and examination as described in this Affidavit and Attachment B.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

48. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT DEVICE, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

49. *Probable Cause.* I submit that there is probable cause to believe records will be stored on the SUBJECT DEVICE, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

51. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a SUBJECT DEVICE for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the SUBJECT DEVICE, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time at a specific location could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and

its data. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

52. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

53. Based on the forgoing, I submit that this affidavit supports probable cause for a warrant to seize and search the SUBJECT DEVICE described in Attachment A for evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252A and 2251A, further described in Attachment B.

54. Further, because of the circumstances discussed in the probable cause section of this affidavit regarding TANNER's unknown vehicle of transportation and lack of consistent residence, I respectfully request that agents executing this warrant be authorized to seize the SUBJECT DEVICE wherever it may be located including from TANNER's person, and/or any vehicle the agents physically observe TANNER enter/exit immediately prior to the execution of this warrant which would provide the agents with probable cause to believe that TANNER has stored the SUBJECT DEVICE therein.

Respectfully submitted,

Melvin Gonzalez
Special Agent, FBI

Subscribed and sworn to in accordance with
Fed. R. Crim. P. 41 by telephone on June 25, 2021.

/s/ MRC

Mark Colombell
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

SUBJECT DEVICE

An Apple iPhone 11 Yellow 64GB, IMEI 356547109384289. Agents executing this warrant are authorized to seize the SUBJECT DEVICE wherever it may be located, including from the person of Jessica L Tanner and/or any vehicle the agents physically observe TANNER enter/exit immediately prior to the execution of this warrant which would provide the agents with probable cause to believe that TANNER has stored the SUBJECT DEVICE therein.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. §§ 2251, 2251A and 2252A relating to the production, distribution, receipt and possession of child pornography and the buying and selling of children, including:

   a. Any and all visual depictions of minors;

   b. Any and all address books, names and lists of names and addresses of minors;

   c. Any and all contracts, diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors; and

   d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

2. For the SUBJECT DEVICE:

   a. Evidence of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

   b. Evidence of software that would allow others to control the SUBJECT DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. Evidence of the lack of such malicious software;

   d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICE.

   e. Evidence of the times the SUBJECT DEVICE was used;

   f. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE;

   g. Records of or information about Internet Protocol addresses used by the SUBJECT DEVICE;

   h. Records of, or information about, the SUBJECT DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

   i. Contextual information necessary to understand the evidence described in this

attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team

and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.

During the execution of the search of the SUBJECT DEVICE described in Attachment A, law enforcement personnel are authorized to: 1) press or swipe the fingers (including thumbs) of any individual, who is reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s); and/or 2) hold the device(s) in front of the face those same individuals and activate the facial recognition feature,, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.